

## REMARKS

Applicant respectfully requests reconsideration and allowance of this application in light of the remarks to follow. Claims 1-30 are pending. By this Amendment, claims 1, 17, 18 and 20-30 have been amended for improved clarity, consistency, and to correct typographical errors; but not for any reasons with regard to the patentability of the recited subject matter.

### Rejection of Claims 21, 22 & 26 Under 35 U.S.C. § 112, Second Paragraph

Claim 21 was rejected under 35 U.S.C. § 112, second paragraph as allegedly being indefinite. The Examiner asserts, "the claim does not set forth any steps involved in a method/process, it is unclear what method/process applicant is intending to encompass." (Office Action, p. 2, ¶ 5, *emphasis added*.) Apparently, the Examiner believes the "operative to" language included in claim 21 fails to positively recite some of the claim's features.

The Examiner has apparently misinterpreted the claim 21 as reciting a method. (Office Action, p. 2, ¶ 5.) To the contrary, Applicant's claim 21 recites, a "system for transmitting a file to a device," in which some of the features recited are functional limitations. A functional limitation defines something by what it does, rather than by what it is. (MPEP § 2173.05(g).) There is nothing inherently wrong with defining some part of an invention in functional terms. (*Id.*) Functional language does not, in and of itself, render a claim improper. (*Id.*) A functional limitation must be evaluated and considered, just like any other limitation of the claim, for what it fairly conveys to a person of ordinary skill in the pertinent art in the context in which it is used. (*Id.*, *emphasis added*.)

In claim 21, the "operative to" language sets forth functional features of Applicant's claimed system. The recitations following the "operative to" of each element are positively and properly recited with respect to the functions of the corresponding claim elements. Moreover, the functional limitations are neither optional nor merely descriptive of the

elements' intended use or result. (See MPEP § 2114.) Accordingly, claim 21 satisfies the requirements of 35 U.S.C. § 112, second paragraph. Applicant, therefore, respectfully requests that the Examiner reconsider and withdraw the rejection of claim 21 under Section 112.

Claims 22 and 26 have been amended to address the concerns raised by the Examiner. (Office Action, p. 3, ¶ 7.) Accordingly, Applicant requests withdraw of the rejection of claims 22 and 26 under 5 U.S.C. § 112, second paragraph.

Rejection of Claim 21 Under 35 U.S.C. § 102(b)

Applicant respectfully traverses the rejection of independent claim 21 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,226,618 to *Downs et al.* ("*Downs*") because *Downs* fails to disclose each and every element recited in the claim. (See MPEP § 2131.) Applicant's claim 21 recites, *inter alia*, "a content server operative ... to communicate with via a secure channel ... and a payment server ... communicating therewith via the secure channel, further operative to provide a shared secret in plaintext form via the secured channel from [a] user to the content server" (emphasis added). The Examiner concedes that *Downs* fails to disclose a "secure channel," as recited in Applicant's claim 21. (Office Action, pp. 9:7-8, 10:13-14, 12:9-10.) Thus, *Downs* cannot anticipate claim 21. Accordingly, the Applicant requests that the Examiner reconsider and withdraw the rejection of claim 21 under Section 102.

The Examiner apparently did not consider the "secure channel" recited in claim 21 because the Examiner believes this features are indefinite under 35 U.S.C. § 112, second paragraph and not positively recited in the claim. (Office Action, p. 2, ¶ 5.) However, as Applicant has already pointed out above, the Examiner's rejection of claim 21 under Section 112 is improper and, thus, the above-noted claim elements must be considered. (See *supra*.)

Rejection of Claim 30 Under 35 U.S.C. § 102(b)

*Downs* cannot support a rejection of Applicant's independent claim 30 under 35 U.S.C. § 102(b) because the reference fails to disclose "means for transmitting, after receipt of an authorization, a decryption key encrypted using the identifier" (emphasis added), as recited in claim 30. (See M.P.E.P. § 2131.) In *Downs*, End-User Device 109 sends an Order SC 641 to Clearinghouse 105. (*Downs*, cols. 23:57-24:4.) Order SC 641 includes, amongst other information, a Public Key 661 of End-User Device 109. (*Id.*) Upon receipt of Order SC 641, Clearinghouse 105 performs several verifications. (*Downs*, col. 24:16-32.) If the verifications are successful, Clearinghouse 105 builds and transfers a License SC 660 to End-User Device 109. (*Downs*, col. 24:33-46.) License SC 660 includes a Symmetric Key 623 and Transaction Data 642 encrypted using Public Key 661 of End-User Device 109.

The Office Action is unclear as to what elements disclosed by *Downs* the Examiner believes correspond to Applicant's claim features. As best Applicant can understand the Office Action, the Examiner asserts that End-User Device 109, Order SC 641 and Symmetric Key 623 correspond to Applicant's claimed "device," "encrypted file" and "identifier," respectively. However, *Downs* does not disclose that License SC 660, including Symmetric Key 623, is transmitted after receiving authorization. Clearinghouse 105 merely verifies that Electronic Digital Content Store 103 is authorized based on information maintained within Clearinghouse 105. (*Downs*, col. 24:19-22.) Thus, *Downs* Clearinghouse 105 does not receive authorization. *Downs*, therefore, does not disclose means for transmitting, after receipt of an authorization, a decryption key encrypted using the identifier" (emphasis added), as recited in Applicant's claim 30. Accordingly, *Downs* cannot support a rejection of claim 30 under 35 U.S.C. 102(b).

Rejection of Claims 18, 19, 24 & 25 Under 35 U.S.C. § 103(a)

*Downs* cannot support a rejection of Applicant's independent claim 18 under 35 U.S.C. § 103(a) because the reference fails to disclose or suggest all the features recited in

the claim. (See M.P.E.P. § 2143.) End-User Device 109 purchases Content 113 from Electronic Digital Content Store 103. (*Downs*, col. 23:15-20.) During this transaction, End-User Device 109 provides Public Key 661 to Electronic Digital Content Store 103. (*Downs*, col. 33:33-38.) Subsequently, End-User Device 109 receives a License SC 660 from Clearinghouse 105 and decrypts a Symmetric Key 623 received from Clearinghouse 105. End-User Device may then receive Content 113 from Content Hosting Site 111.

The Examiner apparently asserts that Electronic Digital Content Store 103 and Content 113 correspond to the claimed "content server" and "encrypted content." (Office Action, p. 5, ¶ 13.) Applicant disagrees. Claim 18 recites "downloading, from the content server, encrypted content." In *Downs*, however, Content Hosting Site 111, not Electronic Digital Content Store 103, provides Content 113 to End-User Device 109. (*Downs*, col. 24:48-54; FIG. 6, step 608.) Thus, *Downs* fails to disclose or suggest "downloading, from the content server, encrypted content," as recited in Applicant's claim 18.

In addition, *Downs* does not disclose or suggest "sending an encoded content download confirmation value to the content server via the insecure communications channel," as recited in claim 18. This feature is not clearly addressed in the Office Action; however, it appears that the Examiner alleges that this feature is suggested by *Downs*' disclosure of an "end-user verif[ying] the received content and transmits a result back to the content host." (Office Action, p. 5, ¶ 15, last two lines on page.)

To the contrary, *Downs* computes a "content digest" and, if this digest is not valid, a sender is notified. (*Downs*, col. 16, steps 415-416.) But *Downs* only sends an error notification to Content Hosting Site 111 in case of an incorrect content digest. *Downs* does not disclose or suggest "sending an encoded content download confirmation value to the content server" (emphasis added), as recited in claim 18. Thus, *Downs* also does not disclose or suggest the above-noted feature of claim 18.

Since *Downs* does not disclose or suggest Applicant's claimed "content server" or "confirmation value." the Examiner has not established a *prima facie* case for rejecting claim 18. Accordingly, Applicant request that the Examiner reconsider and withdraw the rejection of claim 18 under 35 U.S.C. § 103(a).

Claim 24, although of different scope than claim 18, recites features similar to those recited in claim 18. Accordingly, *Downs* cannot support a rejection of claim 19 for similar reasons to those stated above with regard to claim 18.

Claims 19 and 25 depend from claims 18 and 24 respectively. Thus, *Downs* cannot support a rejection of claims 19 and 25 at least due to their respective dependency from claims 18 and 24.

Rejection of Claims 1-7, 20, 22, 23 and 26-29 Under 35 U.S.C. § 103(a)

Applicant traverses the rejection of independent claim 1 under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Downs* in view of U.S. Patent No. 6,226,618 to *vanHeyningen et al.* ("*VanHeyningen*"). Claim 1 recites a combination of features including, "receiving a confirmation authorizing release of a decryption key; and sending the decryption key to the device for decryption of the encrypted content." The Examiner appears to assert that these features are taught by *Downs*' disclosure of "[a]fter verifying the authenticity of the order SC and the transaction SC, the clearinghouse encrypts the content key with the public key of the end-user device for transmission to the end-user device." (Office Action, pp. 8:21-9:4.) Applicant disagrees.

*Downs* says nothing with regard to "receiving a confirmation authorizing release of a decryption key," as recited in Applicant's claim 1. The Examiner apparently asserts that *Downs*' alleged "verifying the authenticity" corresponds to Applicant's claimed "confirmation." (Office Action, pp. 8-9.) However, Clearinghouse 105 merely verifies that Electronic Digital Content Store 103 is authorized based on information maintained within Clearinghouse 105.

(*Downs*, col. 24:19-22; 44:23-36.) Because the Clearinghouse 105 itself verifies that Electronic Digital Content Store 103 is authorized, Clearinghouse does not receive an authorization. *Downs*, therefore, does not disclose "receiving a confirmation authorizing release of a decryption key" (emphasis added), as recited in Applicant's claim 1.

*VanHeyningen* does not overcome *Downs*' deficiencies. The Examiner cites *VanHeyningen* for its alleged disclosure of "using a secure channel." (Office Action, p. 9.) However, *VanHeyningen* does not disclose or suggest the above-noted feature of claim 1, and the Examiner does not assert that *VanHeyningen* makes such a disclosure. Accordingly, *Downs* and *VanHeyningen*, whether taken individually or in combination, fail to teach or suggest "receiving a confirmation," as recited in claim 1.

In addition, the Examiner concedes that *Downs* fails to disclose or suggest "a secure communications channel," as recited in claim 1. (Office Action, p. 9:7-8.) However, the Examiner alleges that *VanHeyningen* discloses such features. In particular, the Examiner apparently cites *VanHeyningen* for its disclosure of a secure socket layer (SSL). (Office Action, p. 9:9-14.) Apparently the Examiner is attempting to provide evidence that secure network connections are known. However, simply showing that secure channels are known is not sufficient to not teach or suggest Applicant's claim 1.

Claim 1 recites, "receiving, from a device, via the insecure communications channel, at least one shared secret; "transmitting encrypted content, via the insecure communications channel to the device; [and] receiving the shared secret in plaintext form via a secure communications channel" (*emphasis added*), as recited in claim 1. *VanHeyningen*, however, does not disclose or suggest transmitting some information over a secure channel and other information over an insecure channel. Thus, *VanHeyningen* does not disclose or suggest "receiving, from a device, via the insecure communications channel, at least one shared secret; "transmitting encrypted content, via the insecure communications channel to

the device; [and] receiving the shared secret in plaintext form via a secure communications channel" (*emphasis added*), as recited in claim 1. Because *Downs* also fails to disclose the use of insecure and secure channels, *Downs* and *VanHeyningen*, when taken individually or in any proper combination, also fail to teach or suggest the above-noted features of Applicant's claim 1.

Moreover, there would be no motivation to modify the *Downs* in view of *VanHeyningen* in a manner that would teach or suggests all the features of Applicant's claim 1. *Downs*' system is directed to encrypting information for transmission insecure Internet connections. (See, e.g., *Downs*, col. 1:51-64.) *VanHeyningen*, in contrast, only discloses secure channels. *VanHeyningen* does not suggest receiving some information over an insecure channel and other information over a secure channel. Indeed, the purported modification of *Downs* based on *VanHeyningen* would tend to suggest a system in which all channels are secured. Thus, employing secure channels, as allegedly disclosed by *VanHeyningen* tends to teach away from Applicant's claimed system which includes "receiving, from a device, via the insecure communications channel, at least one shared secret" and "transmitting encrypted content, via the insecure communications channel," as recited in claim 1.

Accordingly, one of ordinary skill in the art would have no motivation to modify *Downs* in view of *VanHeyningen* in a manner that would result in Applicant's claimed invention. Indeed, Applicant respectfully submits that selectively making some channels secure to meet the limitations of Applicant's claim would require improper hindsight reconstruction of Applicant's claimed method based solely on knowledge the Examiner gleaned from Applicant's disclosure. Such improper hindsight cannot support a *prima facie* case for rejecting Applicant's claim 1.

For the reasons set forth, the Examiner has failed to establish a *prima facie* case for rejecting claim 1 under 35 U.S.C. § 103(a). Accordingly, claim 1 is allowable over the applied references. Claims 2-7 are allowable at least due to their dependency from claim 1.

Independent claims 20, 22 and 26-29, although of different scope than claim 1, include features similar to those recited in claim 1. Accordingly, claims 20, 22 and 26-29 are allowable for similar reasons to those set forth above with regard to claim 1. Claims 20, 22 and 26-29 are, therefore, allowable over *Downs* and *VanHeyningen*. Claim 23 is allowable at least due to its dependence from claim 22.

Rejection of Claims 8-17 Under 35 U.S.C. § 103(a)

The Examiner rejected claims 8-17 under 35 U.S.C. § 103(a) as allegedly not being patentable over the purported combination of *Downs* and *VanHeyningen* in view of U.S. Patent No. 7,165,181 to *Brickell*.

As noted above with regard to independent claim 1, *Downs* and *VanHeyningen* fail to disclose or suggest, at least, "receiving a confirmation authorizing release of a decryption key" and "receiving, from a device, via the insecure communications channel, at least one shared secret; "transmitting encrypted content, via the insecure communications channel to the device; [and] receiving the shared secret in plaintext form via a secure communications channel." *Brickell* does not overcome these deficiencies of *Downs* and *VanHeyningen*.

The Examiner apparently relies on *Brickell* for its alleged disclosure of hashing a public key with a random number. However, *Brickell* does not disclose the above-noted features of claim and the Examiner does not assert that *Brickell* makes any such disclosure. Thus, when *Downs*, *VanHeyningen* and *Brickell* are taken alone or in any proper combination, they fail to teach or suggest all the features of claim 1. Accordingly, claim 1 is allowable because the applied references cannot support a rejection of claim 1 under 35 U.S.C. § 103(a). Claims 8-17 are allowable at least due to their dependence from claim 1.



**Conclusion**

For the reasons set forth above, Applicant respectfully requests allowance of claims 1-30. In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicant's undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge the necessary amount to Deposit Account No. 08-2025 .

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: November 15, 2007

By: /Steven Ashburn/

Steven Ashburn  
Registration No. 56,636

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620